

# DEPAUL UNIVERSITY

---



## Health Information Security & Privacy

**Category:** Operations

**Responsible Department:** Information Services

**Responsible Officer:** Vice President of Information Services

**Effective Date:** 3/15/2016

---

### Policy Summary

---

This policy is for the protection of personal health information created, received, maintained or transmitted by specific departments of the university that are subject to the security and privacy regulations adopted by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996.

---

### Scope

---

This policy affects the following groups of the University:

- Entire University Community

This policy affects all members of the University Community.

---

### Policy

---

#### A. General

This Health Information Security & Privacy Policy and the Procedures governed by the Chief Privacy Compliance Official implement the organization's obligation to protect the security and privacy of all individually identifiable health information subject to regulation under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law No 104-191 (August 21, 1996). DePaul is subject to said HIPAA obligations as it is a covered entity that creates, receives, maintains and/or transmits personal health information as a health care provider, as part of health plans, and/or in other related roles involving health information, within the areas identified as the health care components of the organization.

HIPAA security and privacy regulations establish a number of individual rights with regard to personal health information, including an individual's right to file complaints concerning the entity's compliance with the privacy regulations. DePaul University takes HIPAA security and privacy regulations and complaints thereunder very seriously and will fully investigate and review each

complaint via the complaint procedures outlined herein. Retaliation against any individual filing a complaint about the privacy practices of DePaul is prohibited.

## **B. University Chief Privacy Compliance Official**

The President or Officer with authority delegated by the President shall designate an appropriately qualified member of the University staff to serve as the Chief Privacy Compliance Official to implement the Procedures as a matter of sound business practice, to protect the interests of our community and to fulfill our legal obligations under HIPAA and its implementing regulations at 45 Code of Federal Regulations Parts 160 and 164 (Security and Privacy Rules).

## **C. Hybrid Designation**

The Chief Privacy Compliance Official shall designate appropriate departments and subdivisions of departments to be identified as part of the Health Care Component of the university that will process and maintain protected health information subject to the Security and Privacy Rules. Activity conducted outside of the University's designated Health Care Component shall not include the creation, use, maintenance, or transmission of any protected health information subject to the Security and Privacy Rules without review by the Chief Privacy Compliance Official.

All faculty members, employees, and agents of the University are obligated to follow this Health Information Security and Privacy Policy and the corresponding procedures. Failure to do so can result in fines or penalties to the University and can be grounds for disciplinary action, including termination of employment, as well as potential criminal penalties.

## **D. Procedures**

Each specifically identified and designated department shall establish procedures for the department or subdivision of the department to implement this policy when creating, receiving, maintaining, transmitting, and/or disclosing personal health information subject to and consistent with state and federal laws and regulations.

## **E. Questions**

For questions about any use or disclosure of individually identifiable health information or about other obligations under this Health Information Security and Privacy Policy, departmental procedures for the protection of personal health information, the Security and Privacy Rules, or other related federal or state laws, consult the Chief Privacy Compliance Official or appropriate department designee for privacy compliance assistance.

---

## **Procedures**

---

Specific departmental procedures regarding the protection of personal health information when such information is created, received, maintained, transmitted, and/or disclosed will be developed by the individual component departments and the Privacy Compliance Officials.

Procedures for filing a Complaint regarding DePaul University's privacy practices and compliance with the HIPAA Privacy Regulations (45 Code of Federal Regulations Part 164, Subpart E) are outlined below:

A written complaint may be filed with the university and/or it may be sent to the Office for Civil Rights, in the Department of Health and Human Services @ <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>

The DePaul University HIPAA complaint process is initiated by filing a HIPAA Complaint Report with the Chief Privacy Compliance Official. The report should include a description of the complaint, the persons/department involved and the desired outcome or action needed to resolve the issue. The Chief Privacy Compliance Official will acknowledge receipt of the complaint to the complainant in writing, or for verbal complaints, by telephone, and relay the information to the relevant covered component area. A resolution or response plan will be developed, documented in writing and relayed to the appropriate parties, including the complainant, by the Chief Privacy Compliance Official.

The Chief Privacy Compliance Official will maintain a record of all complaints received, the date(s) of university action in response to the complaint, the disposition of the complaint and the action(s) taken, if any. If, in response to a complaint, sanctions against members of the workforce are administered for failure to comply with university policies, procedures or regulations, a record of the sanction will similarly be created and maintained by the Chief Privacy Compliance Official.

Complaints must be filed within 180 days of when the complainant knew that the act or omission complained of occurred. The 180-day filing period may be extended if the complainant can show 'good cause'. Any alleged violation must have occurred on or after April 14, 2003.

---

## **Divisional Collaborations**

---

Office of the General Counsel  
Internal Audit  
Human Resource Benefit Administration  
Family and Community Services  
Athletics  
Student Affairs  
Institutional Review Board  
Ray Meyer Recreation Center

---

## **Contact Information**

---

**Chief Privacy Compliance Official**  
Vice President of Information Services  
Bob McCormick  
(312) 362-8200 Phone  
(312) 362-8097 Fax  
[bmccormi@depaul.edu](mailto:bmccormi@depaul.edu)

---

## **Appendices**

---

### **Legal basis:**

Health Insurance Portability and Accountability Act of 1996, Pub Law No 104-191 (Aug 21, 1996).  
45 Code of Federal Regulations Parts 160 and 164 (Security and Privacy Rules) (Aug 14, 2002)

---

## **History/Revisions**

---

Origination Date: 04/07/2003

Last Amended Date: 03/15/2016

Next Review Date: N/A